In the Claims

1.(Amended) A method for testing an integrated circuit containing hardware and/or software parts having a confidential nature, using a tester, wherein this method comprises the steps of:

- in said integrated circuit:

generating a random number by a generator,

ciphering this random number using a key stored in said integrated circuit via a ciphering algorithm to obtain a first password placed in a password register, and

sending the random number to said tester,

- and, in said tester:

ciphering in parallel said random number received using a key identical to that used in said integrated circuit via an identical ciphering algorithm to that implemented in said integrated circuit, to generate a second password, and

sending said second password from the tester to said integrated circuit,

- then, in said integrated circuit,

comparing said first and second passwords by comparing means,

freeing a test path leading from said tester to said parts of a confidential nature by opening a barrier in the integrated circuit, only if the comparison establishes a match between said first and second passwords, and

effecting the test of said elements of a confidential nature.

2. (Original) A method according to claim 1, wherein it also comprises the steps of :

- in said integrated circuit:

ciphering said random number using said key stored in the integrated circuit via said ciphering algorithm to obtain a third password;

sending said third password to said tester; and

- in said tester:

ciphering said random number received using said key stored in said tester via said ciphering algorithm to obtain a fourth password;

comparing said third and fourth passwords; and

authorizing the ciphering of said second password via said tester only if there is a match between said third and fourth passwords.

3. (Original) A method according to claim 1, wherein it also comprises the steps of :

- in said integrated circuit:

ciphering said random number using said key stored in the integrated circuit via said ciphering algorithm to obtain a third password;

sending said third password to said tester; and

- in said tester:

performing the reverse ciphering of said third password received, using said key stored in said tester via said ciphering algorithm to find a calculated random number;

comprising the random number received from said integrated circuit to said calculated random number, and

authorizing the ciphering of said second password via said tester only if there is a match between said received and calculated random numbers.

4. (Original) A method according to claims 2 or 3, wherein the ciphering of said third and/or fourth passwords is made on the basis of a different number of clock strokes than that used for ciphering said first and second passwords.

5. (Original) A method according to claim 1, wherein it consists, as far as said matches are concerned, in checking that said passwords; respectively said received and calculated random numbers are equal.

6. (Original) A method according to claim 1, wherein it comprises the steps of, upon manufacturing said integrated circuit, storing a predetermined value of said cipher key, and during execution of said test procedure using said tester, sending to said integrated circuit, a cipher key value, checking whether said cipher key sent has the predetermined value stored in said integrated circuit, commanding said key sent to be stored in said integrated circuit in case an inequality is observed during said check and blocking in such case the storage in said circuit of any other cipher key.

7. (Amended) An integrated circuit including hardware and/or software parts having a confidential nature and means for conditionally routing test data to said hardware and/or software parts, wherein it includes:

- a random number generator;
- means for storing a cipher key;
- processing means for calculating a first password from said key and a generated random number, using a cipher algorithm;
- means for routing a random number towards the exterior; and
- means for comparing said first calculated password placed in a password register with a second password received from the exterior, said second password being calculated in accordance with the random number generated by the generator, said comparison means being connected to said routing means for freeing a test path leading to said parts of a confidential nature by opening a barrier in the integrated circuit [so as to make them transparent to said test data] only if [they observe] there is a match between said first and second passwords.

8. (Amended) An integrated circuit according to claim 7, wherein [it includes means for storing said first calculated password, said storage means being] said password register is placed before the comparison means to provide [them] said first stored password, for comparison means, at the moment of comparison with the second password.

9. (Original) An integrated circuit according to claim 7, wherein the means for storing the cipher key are an EEPROM memory which also includes a redundancy unit check.

10. (Original) An integrated circuit according to claim 7, wherein the processing means are provided for calculating a third password using the cipher key, from the random number generated and the circuit cipher algorithm, said third password being intended to be sent towards the exterior with the random number to a specific tester.

11. (Original) A tester for integrated circuits including hardware and/or software parts having a confidential nature, this tester including means for effecting a proper working test of said hardware and/or software parts to route the corresponding data to said circuit, wherein it includes:

- means for receiving a random number generated by an integrated circuit to be tested;

- means for storing a cipher key;
- processing means for calculating a second password from said cipher key and from the received random number, using a cipher algorithm, and
- said processing means being connected to said routing means for sending said second calculated password to said integrated circuit.

12. (Original) A tester according to claim 11, wherein said processing means are also arranged to calculate, using a cipher algorithm, a fourth password from said cipher key and from the received random number;

wherein said means for receiving said random number are also arranged to receive a third password calculated in said integrated circuit, and

wherein it also includes comparison means to check the match between said third received password and said fourth calculated password, said processing means only being authorised to calculate said second password if the comparison means observe a predetermined match between said third and fourth passwords.

13. (Original) A tester according to claim 11, wherein:

- said means for receiving said random number are also arranged to receive a third password calculated in said integrated circuit, and
- said processing means are also arranged to recalculate a random number using a reverse cipher algorithm, and from said third password calculated in said integrated circuit and from said cipher key; and

wherein it also includes comparison means for checking the match between said received random number and said calculated random number, said processing means only being authorised to calculate said second password if the comparison means observe a predetermined match between said random numbers.

14. (New) A method according to claim 1, wherein, when tester is connected to integrated circuit, the test procedure is initiated by sending the test mode signal form the tester, which causes the introduction in a processing unit of the random number generated, at the instant concerned, by a random number generator, and a cipher key from storing means, and the transmission of said random number to said tester.

15. (New) An integrated circuit according to claim 7, wherein the barrier for accessing to the confidential parts of the integrated circuit includes two multiplexers connected between routing means and a confidential section, one of the multiplexers being controlled to authorize the passage of test data from routing means only if a control signal is supplied by a comparator of comparing means in function of a match between said first and second passwords.